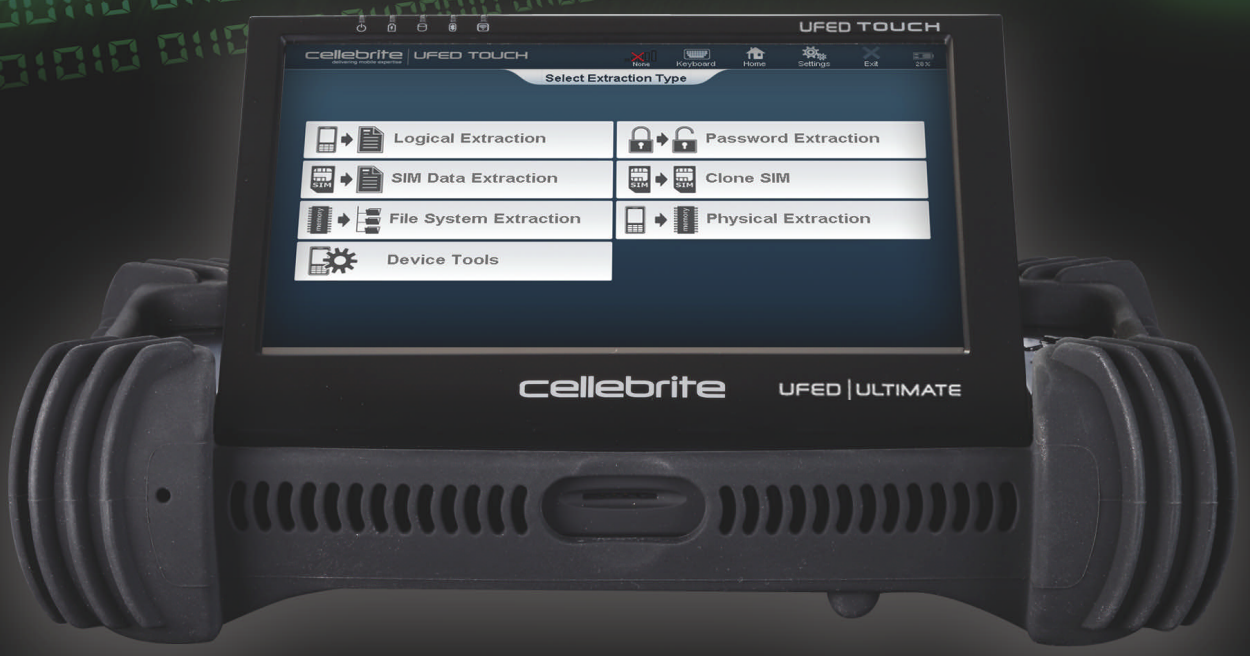
THE KEYS TO MOBILE DEVICE ANALYSIS



Deep data extraction, thorough decoding, and accurate reporting all open the door to a forensically sound mobile device examination process that supports any investigation.

The Cellebrite UFED Series hardware and software together offer this trilateral solution to the investigative challenge posed by a multitude of mobile devices, capabilities, and information.

cellebrite
delivering mobile expertise

UFED series

THE KEYS TO MOBILE DEVICE ANALYSIS

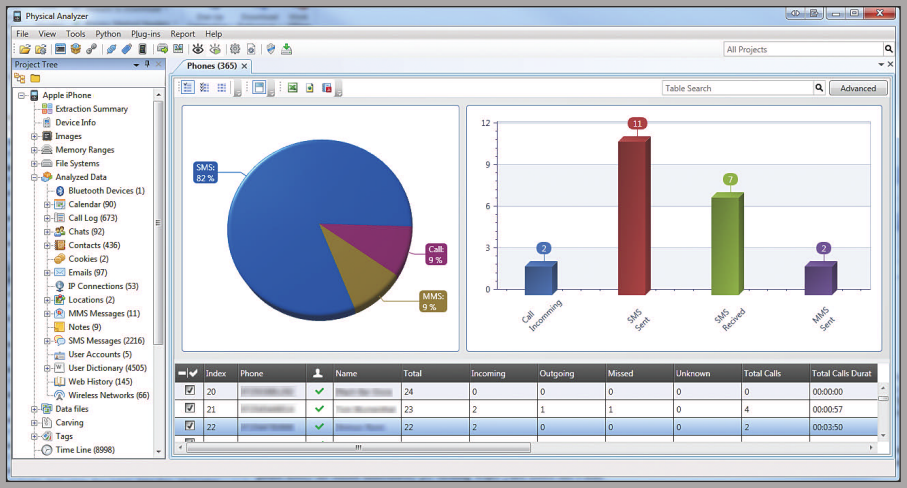
Success in any investigation relies on having the right tool for the job. This means not only finding a solution that can accurately perform the functions required, but also one that streamlines the process, allowing you to work quickly and efficiently. Investigations involving mobile devices make this particularly crucial, as they involve large amounts of data, much of which is most useful if discovered in the earliest stages of an investigation. For this reason it is important to find a tool that allows you to extract as much data as possible from any mobile device and then analyze it in a way that quickly turns gigabytes of raw data into actionable evidence.

Cellebrite's Universal Forensic Extraction Device (UFED) Series brings together these key traits enabling advanced extraction, decoding, analysis, and reporting of mobile data.

Extraction

Upon seizure, extraction is the most important step in mobile phone analysis. Aside from the obvious fact that the data must be extracted before it is analyzed, the extraction method has a great bearing on due process and the proper preservation of evidence. If the data is incorrectly handled in this early stage, the entire case is compromised. The UFED can extract data from all makes and models including Samsung, Nokia, Apple, LG, BlackBerry and many others running Android, iOS, Windows, and other operating systems. It can also neutralize, break, or bypass passwords/passcodes on many of these models, giving you access to the devices' complete contents.

The UFED Ultimate, which enables file system and physical as well as logical extractions, can work with an optional add-on, UFED CHINEX, a generic solution to cope with clone devices made with Chinese chipsets. The inconsistent techniques used to manufacture these devices can make it difficult to predict which components and operating systems they may be running. UFED CHINEX automatically detects the presence of these chipsets and whether it's possible to extract data from the devices.



Project analytics can help illustrate the device user's activities.

UFED Physical Analyzer

As mobile devices become more complex, the sheer volume of raw data they hold becomes unmanageable on its own. The UFED Physical Analyzer provides tools to make this data more actionable so you won't find yourself reading through thousands of disconnected messages and phone calls. First, investigators can create watch lists relating to specific types of cases. The watch list consists of key words that are critical to an investigation. For example, in drug cases, a watch list may contain words like "drug" or it may contain common slang such as "salts" or "angel". Words can be set to appear in specific colors, making them easier to spot and sort.

The chronology of events can reveal valuable information about the data and establish correlating links between calls or messages. The Timeline tool, available in both UFED Physical Analyzer and UFED Logical Analyzer, allows investigators to harness this information by zeroing in on a specific time or date range. In a kidnapping case, for example, the investigator can focus on the time preceding or surrounding the kidnapping. The Timeline tool can even exclude times in which the suspect or victim's whereabouts are known, such as work days. Types of events (calls, SMS messages, images sent, etc.) can be filtered out based on the investigator's needs.

Project analytics can help create a picture of the device user's activities. It can chart the types of activities performed on the device as well as their frequency. It can also illustrate who the user interacted with and how. Were the interactions one sided or did the contact reply? Was contact established using one form of communication over the other? This tool can help form a

Training

With so many tools available in the UFED Series, it's easy to overlook the investigative capabilities they make available. Cellebrite's individual and group training can help you put these tools' full range of benefits to use. Training also helps you understand how the tools work and what's going on "under the hood," which can be important in courtroom testimony.

picture of the device user's habits and create a list of his or her most frequent contacts, narrowing down a list of possible suspects.

Smartphones also provide a wealth of location information, be it from maps, apps that "check in" to a location, or connections to Wi-Fi hotspots. UFED Physical Analyzer's location tool allows the investigator to access this data, creating a record of the user's movements. This information can even be imported into Google Earth as a video "flyover" creating an excellent visual. This video can be used as an exhibit during trial or during the investigation to locate additional evidence in locations that hadn't previously been linked to the user. (Note: not every single hotspot or map will lead to anything of evidentiary value.)

Data found on the device being examined can often lead to other sources. Especially in the case of smartphones from which a variety of applications can be accessed, the trail may move off the device and into social media. iPhones allow users to create a keychain containing login information for all of their applications, information that becomes available to the analyst once the UFED has extracted the data. This allows the analyst to move the investigation to the next step, seeking consent or a warrant to search social media evidence, for example, without delays.

Documentation is a crucial step in any investigation, and UFED analytical software makes this easier by allowing the analyst to bookmark specific data and insert notes throughout the investigation. These notes can then be included in the final report or not, depending on the investigator's preference. Also useful to the reporting process is the UFED Reader application which can be downloaded for free to allow the investigator to collaborate with a supervisor or attorney who does not have UFED. Reports, images, and notes can be exported, allowing a third party to view them as the investigator sees them.

The wide variety of tools provided by the UFED Series allows the investigator to quickly drill down to the critical evidence without wasting hours poring through raw data. When mobile device evidence is actionable, the power to move ahead on cases is back in the investigator's hands. To this end, Cellebrite maintains a regular schedule of updates, which enable it to incorporate customer feedback in making continued improvements to the UFED product line.

From the Front Line

Detective Bob Elder of the Victoria Police Department Computer and Mobile Phone Forensics Unit has been using the UFED series for over six years now and the UFED Touch for the past 3 months. "The new Touch is a beautiful piece of equipment, I am a very big fan," he says.

He chose the UFED products for their features as well as Cellebrite's support services. "Cellebrite focuses on the higher levels of acquisitions (file system and physical) with their products. They do a very good job with the logical acquisition like other tools but their real strength lies in file system and physical data dumps; not only in the acquisition process but in the decoding or conversion process from the RAW data dump to a readable format," Detective Elder says.

"The team at Cellebrite actively monitor LEO list servs, proactively seek out problem phones that we are facing, respond to questions in a professional manner, and work with advanced users who are conducting R&D to improve their product support."

Locked or encrypted Blackberry's are massive challenge to police (and probably others around the world), Elder noted. "In one of our major drug files, one of the main players had been using a Blackberry that was password locked and had the encryption activated. Having the capability to conduct chipoff acquisitions, we were able to remove the chip from the board, prepare it for a read, read the full RAW data using the supported programmer/adapter, and then place this RAW dump into the Physical Analyzer software and let the Plugins do their thing."

"The software was able to determine the encryption type, provide us with the information we needed to decrypt the device, and recover the user data. Having access to this damaging user data was very beneficial to our case. It is the only tool that I know of that will allow us to recover all this user data."

Link Analysis

One improvement is a new application, UFED Link Analysis. When an investigation includes multiple extractions, Link Analysis helps investigators establish the connections between each device. Do the users know each other? How? What contacts do they share? How do their interactions with these contacts compare? Link Analysis helps answer these questions by creating a visual link between the users' contacts and communications. Filters allow the investigator to drill down to the most important connections and analyze them. How did the users communicate, what applications did they use, and what groups do they belong to? UFED Link Analysis allows the investigator to include as much data as is known about each user, create color coded groups of contacts to help visually connect individuals, and compares the names, nicknames, and contact information for each contact from each extraction. These links can prove invaluable in establishing your case. If needed, you can export the results of your analysis to intelligence-building tools that incorporate your mobile data into much larger datasets from multiple sources.

The key to any investigation is choosing the right tool for the job. When analyzing mobile devices, it is essential that your tool give you full access to the data in the extraction and then allow you to quickly and accurately sift through this data with tools that make the data actionable.

cellebrite

delivering mobile expertise

SAME TRUSTED UFED
MORE ACTIONABLE DATA

Extract, View, and Act with Cellebrite's UFED Series

Cellebrite UFED sets the industry standard in mobile forensics by allowing you to:

EXTRACT: Conduct a faster, more streamlined extraction with UFED Touch

VIEW: Translate raw device data into rich, actionable information

ACT: Pinpoint leads and other potential sources of evidence

The Cellebrite UFED Series has a unique feature set that provides you with:

- The only mobile forensics solution to deliver physical extraction and decoding of all three major smartphone platforms: Android™, iOS® and BlackBerry®
- Robust analytics to reveal better leads through connections and patterns
- Proprietary hardware, software, and bootloaders that ensure a forensically sound investigation every time

Learn more about the industry leading Cellebrite UFED: http://bit.ly/TuDtZ2

1.888.853.0030
forensicsales@cellebriteusa.com
www.facebook.com/CellebriteUFED
@CellebriteUSA

cellebrite
delivering mobile expertise

UFED series

All information included herein, such as text, graphics, photos, Cellebrite's logo and images, is the exclusive property of Cellebrite and protected by United States and international copyright laws. Other brand names and logos may be trademarks or registered trademarks of others.